МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник тез доповідей
Всеукраїнської науково-практичної студентської конференції

(16 жовтня 2024 року, м. Харків, Україна)

Електронний ресурс

Харків – 2024

УДК 004.056.53

Оченашко М. О.
здобувач ступеня доктора філософії,
Харківський національний університет радіоелектроніки
Науковий керівник
Гороховатський В.О.
д.т.н., професор, професор кафедри інформатики,
Харківський національний університет радіоелектроніки

ВПЛИВ GDPR НА ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ

Персональні дані користувачів використовуються більшістю сервісів, від соціальних мереж до охорони здоров'я та фінансових послуг. Ці дані, у більшості випадків, необхідні для надання різноманітних послуг. Оскільки компанії продовжують накопичувати величезні обсяги даних, вони стикаються зі зростаючим тиском щодо їх захисту не тільки для збереження своєї репутації, але й для дотримання суворих правових норм, таких як Загальний регламент про захист даних (GDPR).

GDPR, запроваджений у 2018 році, встановив суворіші вимоги щодо захисту даних, конфіденційності та безпеки. Згідно з регламентом, компанії зобов'язані впроваджувати відповідні технічні та організаційні заходи для забезпечення безпеки персональних даних, включаючи методи шифрування, токенізації, та псевдонімізації [1, 2].

Одним із ключових методів забезпечення відповідності GDPR та зменшення ризику витоку даних є токенізація. Замінюючи конфіденційні дані унікальним ідентифікатором або «токеном», компанії можуть ефективно захистити особисту інформацію, зберігаючи при цьому можливість використовувати її в операційних цілях. Токенізація змінює спосіб роботи з даними, мінімізуючи ймовірність витоку в разі кібератаки або злому.

Загрози для корпоративного інформаційного середовища. Інформаційне середовище, що складається з цифрових систем, які зберігають, обробляють і передають дані, стикається зі зростаючим набором загроз з розвитком технологій. Вразливості «нульового дня» становлять значні ризики, оскільки вони включають невідомі недоліки безпеки, якими користуються зловмисники до того, як з'являються патчі. Інсайдерські загрози ще більше ускладнюють безпеку, оскільки співробітники або підрядники можуть ненавмисно або навмисно скомпрометувати конфіденційну інформацію. Ці різноманітні загрози вимагають багаторівневого підходу до безпеки і забезпечення захисту даних користувачів.

Токенізація даних. Токенізація – це ефективний метод підвищення безпеки даних та забезпечення дотримання GDPR. Вона передбачає заміну конфіденційних даних, таких як персональні дані (PII), неконфіденційним еквівалентом, який називається токеном. Цей токен не має ніякої цінності або

значення поза конкретною системою, де він створюється і управляється, що робить його марним для зловмисників, якщо його перехоплять. На відміну від деяких видів шифрування, які допускають розшифрування за допомогою правильного ключа, токенізація повністю видаляє конфіденційні дані з системи компанії, зменшуючи ризики витоку.

Оскільки токени не вважаються персональними даними відповідно до GDPR, організації можуть токенізувати конфіденційні дані, продовжуючи використовувати токени для внутрішніх операцій, таких як аналітика, обслуговування клієнтів або обробка транзакцій, не порушуючи GDPR. Конфіденційна інформація зберігається окремо і безпечно, що мінімізує ризики, пов'язані з витоком даних або зловживанням ними [3].

Навіть якщо зловмисник отримає доступ до баз даних компанії, токени, які він знайде, не матимуть сенсу без доступу до відповідних даних, що зберігаються у сховищі токенів. Таке утримання конфіденційної інформації значно знижує ризик порушень GDPR, оскільки витік токенів не прирівнюється до витоку персональних даних [5]. Оскільки токени легко від'єднуються від конфіденційних даних, які вони представляють, організації можуть видалити персональні дані користувача за запитом без необхідності пошуку в декількох системах, що спрощує дотримання цього аспекту GDPR. Таким чином, токенізація мінімізує ризики витоку конфіденційних даних, зменшує обсяг регуляторного нагляду та спрощує управління персональними даними [4].

Приклад 1. Токенізація даних у фінансових організаціях. У секторі фінансових послуг захист конфіденційних платіжних даних є головним пріоритетом через високий ризик шахрайства та крадіжки персональних даних. Банки та фінтех-компанії щодня обробляють величезні обсяги персональної та фінансової інформації, включаючи номери кредитних карток, дані рахунків та історії транзакцій.

Токенізація стала ключовим рішенням для захисту платіжних даних у цій галузі. Замінюючи конфіденційні дані, такі як інформація про власника картки, випадково згенерованими токенами, банки та фінтех-компанії можуть обробляти платежі, не піддаючи оригінальні дані впливу хакерів. Наприклад, під час транзакції номер кредитної картки перетворюється на токен і зберігається в захищеному сховищі, а в процесі оплати використовується лише токен. Це гарантує, що навіть якщо систему буде зламано, викрадені дані не матимуть жодної цінності [1].

Приклад 2. Токенізація даних пацієнтів у сфері охорони здоров'я. Медичні організації керують дуже чутливими даними, включаючи медичні записи, діагнози та історії лікування, що робить їх головними мішенями для кібератак і витоків даних. Замінюючи конфіденційну медичну інформацію унікальними токенами, медичні працівники можуть безпечно зберігати та передавати записи, не розкриваючи реальні дані. Наприклад, під час зберігання записів пацієнтів або обміну ними між медичними установами, токенізовані дані гарантують, що будь-яка перехоплена інформація буде марною для несанкціонованих осіб.

Для токенізації часто використовують різні методи, такі як кодування, хешування, та оцінка інформативності, щоб підвищити безпеку та корисність даних. Хешування додає додатковий рівень захисту, генеруючи незворотні рядки фіксованої довжини з токенізованих даних. Оцінка інформативності гарантує, що токенізовані набори даних зберігають свою аналітичну цінність, залишаючись при цьому сумісними з правилами конфіденційності. [6-9]

Висновок. Загальний регламент про захист даних (GDPR) встановив новий глобальний стандарт конфіденційності даних, змушуючи організації впроваджувати більш ефективні практики безпеки для захисту даних користувачів. Токенізація, зокрема, пропонує високоефективний метод підвищення безпеки та досягнення відповідності вимогам. Замінюючи конфіденційні дані токенами, які не мають сенсу поза захищеною системою, компанії можуть значно знизити ризик витоку даних і мінімізувати ризик витоку особистої інформації.

Впровадження токенізації не тільки забезпечує відповідність суворим вимогам GDPR, таким як псевдонімізація та мінімізація даних, але й надає організаціям практичне рішення для безпечного управління даними в різних галузях. У сфері фінансових послуг, охорони здоров'я чи електронної комерції токенізація допомагає зменшити ризики кіберзагроз, дозволяючи компаніям продовжувати працювати ефективно та безпечно.

Список використаних джерел:

1. Data Sharing Under the General Data Protection Regulation / A. Vlahou et al. Hypertension. 2021. Vol. 77, no. 4. P. 1029–1035. URL: https://doi.org/10.1161/hypertensionaha.120.16340 (дата звернення: 22.09.2024).

2. General Data Protection Regulation (GDPR) Compliance Guidelines. GDPR.eu. URL: https://gdpr.eu/ (дата звернення: 22.09.2024).

3. IBM Minimizing application privacy risk. URL: https://developer.ibm.com/articles/s-gdpr3/ (дата звернення: 22.09.2024).

4. Knutsson M. Compliance with the General Data Protection Regulation: an exploratory case study on business systems' adaptation : thesis. 2017. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-209772 (дата звернення: 23.09.2024).

5. Welch R. GDPR and Tokenizing Data (Part 3 in a Series) | TDWI. TDWI. URL: https://tdwi.org/articles/2018/06/06/biz-all-gdpr-and-tokenizing-data-3.aspx (дата звернення: 22.09.2024).

6. Gorokhovatsky, V. (2014), Structural Analysis and Intellectual Data Processing in Computer Vision, SMIT, Kharkiv, 316 p.

7. Gorokhovatskyi V. Vlasenko N. (2021), The image description reduction in the set of descriptors on informativeness metric criteria base. Advanced Information Systems, 5 (4), 10–16. doi: https://doi.org/10.20998/2522-9052.2021.4.02

8. Гороховатський В.О., Гадецька С.В., Стяглик Н.І. Вивчення статистичних властивостей моделі блочного подання для множини дескрипторів

ключових точок зображень. Радіоелектроніка, інформатика, управління. – 2019. – №2 . – С. 100–107.

9. Y. I. Daradkeh, V. Gorokhovatskyi, I. Tvoroshenko, and M. Zeghid. Improving the effectiveness of image classification structural methods by compressing the description according to the information content criterion. Computers, Materials & Continua 80.2 (2024): 3085-3106.

УДК 339.9; 339.97

Редзюк Є.В.
к.е.н., доцент, старший науковий співробітник
сектору міжнародних фінансових досліджень
ДУ «Інститут економіки та прогнозування НАН України», м.Київ

ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНИЙ ВПЛИВ В СУЧАСНИХ ГЕОПОЛІТИЧНИХ І ГЕОЕКОНОМІЧНИХ ВІДНОСИНАХ

Період 2000-2024 рр. – це епоха світового розвитку може бути охарактеризована як момент біфуркації, як етап переходу від індустріального суспільства до постіндустріального, інформаційного, медійного та орієнтованого на системне оновлення і використання знань. При цьому глобалізація, гармонійність міжнародних економічних відносин та демократичні процеси в світі знаходяться під тиском сучасних проблем, особливо, що стосується в отриманні неупередженої і правдивої інформації, яка під тиском олігархії, охлократії, неефективності державних інституцій суттєво деформується і спотворюється. В цьому аспекті дослідження процесів глобального політичного й економічного розвитку у взаємодії зі створенням інформації та впливом інформації на сучасне суспільство є актуальним та необхідним для більш безпечного і системного розвитку людства.

Визначення геополітики як науки про світову політику, що становить систему знань про контроль над географічним простором обумовлює замислитись про роль інформації та інформаційного забезпечення в цьому процесі. Тому, на наш погляд, необхідно розуміти, що сучасна геополітика – це дієвий зовнішньополітичний інститут держави в розумінні структур, механізмів, інструментів, за допомогою яких різні правлячі еліти певної країни намагаються розділити “зони впливу”, “зони безпеки”, “зони національних інтересів” тощо й у такий спосіб досягти влади та можливості контролю над процесами, що відбуваються на міжкраїнному, регіональному і на світовому рівнях. В той же час у класичному розумінні геополітика як наука – це державна доктрина (вчення, система теоретично обґрунтованих поглядів на суттєво